THE UNITED STATES
CYBER CONSEQUENCES UNIT

The Project for Securing the Electronics Supply Chain

Organized by the Internet Security Alliance

Scott Borg

Director and Chief Economist
U.S. Cyber Consequences Unit

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit. All rights reserved.

The Nightmare: military information systems hardwired with backdoors and logic bombs, so that they could be turned against us

- Not detectable
- Capable of surviving many changes of software
- Set to be triggered by symptoms of serious mobilization
- Not shutting systems down, but using them to actively destroy things

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

The Military’s First Idea of a Solution: produce the electronics in a totally controlled environment

- Carry out all steps domestically
- Carefully vetted personnel
- Constant supervision and surveillance
- Every input inspected
- Every operation verified

The Problem with This Solution: much too expensive to be feasible

- Little resemblance to the way electronics are currently produced
- Not practices a company could institute and remain competitive
- Not even practices the government could afford to pay for

Hence, industry would (have to) walk away
— and even the government would walk away!

The Big New Strategy: solve this customer problem in a way that produces other benefits

- Companies face huge supply chain threats and losses other than malicious firmware:

  Interruptions of supply → delaying production, increasing costs, postponing revenues, losing sales

  Quality control problems → damaging the brand, undermining customer relationships

  Counterfeit products → damaging the brand, losing sales

  Loss of intellectual property → undermining future ability to compete

- A systematic program for dealing with these other threats could hugely reduce the risk of malicious firmware as a by-product!

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

The Tool for Implementing This Strategy: a guidelines document that states the security requirements for each stage of the supply chain

- A declaration of the conditions for doing business with the major electronics companies
- Not just security categories or mere formalities, but actual instructions for securing each supply chain operation
- Requirements that could be individually waved, but only if a prospective business partner could make a case for an alternative requirement
- Security provisions designed to be complementary and to operate collectively

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Private Sector Corporations Have Huge Motivations for Carrying Out this Strategy

- The losses they are currently suffering from supply chain problems are enormous and not at all hypothetical

- They need a way of imposing discipline on their global business partners

- Anti-trust provisions deprive them of other ways of doing this (putting them at a disadvantage vs., e.g., China)

- The companies that are the big players are the ones that are being most hurt by supply chain insecurities

- Seizing the initiative allows these technological leaders to shape everything that will be done in this area

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Four Different Kinds of Damage to Guard Against

I. Interruption of Operations

II. Corruption of Operations

III. Discrediting of Operations

IV. Loss of Control of Operations

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Different Remedies for Different Kinds of Damage

I. Protection against interruption of operations:

- Continual, mandatory sharing of production information across supply chain
- Maintaining alternative sources

II. Protection against corruption of operations:

- Strict control of environments where key intellectual property is being applied
- Logical tamper-revealing seals (hash functions, feature checks)
- Physical tamper-revealing seals (container seals)
- Effective tracking of sealed containers

III. Protection against discrediting of operations (undermining trust):

- Logging of every operation and who is responsible
- Bonded operators and facilities

IV. Protection against loss of control of operations:

- Versioning as a tool for protecting intellectual properties

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Different supply chain stages to which the remedies need to be applied (in each branch of the production flow tree)

I. Design Phase

II. Fabrication Phase

III. Assembly Phase

IV. Distribution Phase

V. Maintenance Phase

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Hence: A “Remedies for Stages” Grid

Strategies & Techniques for Securing Electronics Supply Chains

(BORG/ISA FRAMEWORK)

		REMEDIES			
		1) Protections against the *interruption* of production	2) Protections against the *corruption* of production	3) Protections against the *discrediting* of production	4) Protections against the *loss of control* of production
SUPPLY STAGES	**I. Design Phase**				
	II. Fabrication Phase				
	III. Assembly Phase				
	IV. Distribution Phase				
	V. Maintenance Phase				

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

I. Design Phase

Overall product design

- Specification of electronic inputs and outputs
- Specification of overall physical design features

Detailed product design

- Schematic diagrams using circuit design software
- Physical circuit layouts using circuit layout software
- Physical assembly engineering and design

Creation of production masters

- Wafer mask production
- Creation of prototypes, templates, and molds

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

II. Fabrication Phase

Sourcing of materials & parts

Fabrication processes

- Receiving of materials and parts
- Carrying out of fabrication processes
- Downloading of firmware
- Quality control and verification tests

Shipping of components

- Packaging and sealing of shipments

III. Assembly Phase

Assembly equipment configurations

Assembly processes

- Receiving of parts and materials
- Carrying out of assembly processes

Assembly outputs

- Quality control processes and verification tests
- Packaging and sealing of products

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

IV. Distribution Phase

Transport of finished products

- Large container integrity
- Large container tracking

Distribution of finished products

- Breakdown and forwarding of products

V. Maintenance Phase

After-sale maintenance of product

- Monitoring of product’s operational efficiency

Updates to product

Destruction of used components

Legal relationships necessary between global component suppliers, assemblers, and the overseeing company

1) Rigorous, unambiguous contracts, delineating the security measures

2) Locally responsible corporations with a long term interest in complying

3) Local ways of overcoming agency problems, motivating executives and workers

4) Adequate provision for verifying that security measures are being properly implemented

5) Local enforcement of agreements at all levels

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit

Thank you!

For more information or permission to use this material in its current form, please contact:

Scott Borg
U.S. Cyber Consequences Unit
P.O. Box 1390
Norwich, VT 05055
scott.borg@usccu.us
802 – 649 - 3849

Copyright © 2010 Scott Borg/U.S. Cyber Consequences Unit